UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/522,063 | 03/09/2000 | Joshua Allen | MSI-489US | 4281 |

22801 7590 08/10/2004

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

| EXAMINER | |
|---|---|
| HO, THOMAS M | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2134 | 8 |

DATE MAILED: 08/10/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/522,063 | ALLEN, JOSHUA | |
| | Examiner | Art Unit | |
| | Thomas M Ho | 2134 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *09 March 2000*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-23,26-36,39-44 and 47-50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *15,17,18 and 36* is/are allowed.

6)☒ Claim(s) *1-14,16,19-23,26-35,39-44 and 47-50* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. §§ 119 and 120**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

## DETAILED ACTION

**1. The amendment of 5/5/04 has been received and entered.**

**2. Claims 24-25 have been canceled.**

**Claims 37-38 have been canceled.**

**Claims 45-46 have been canceled.**

**3. Claims 15, 17-18, 36 are allowable.**

### Response To Arguments

As discussed in the telephonic interview of 4/8/04, it is noted that Applicant's claims in which a "token using one-way encryption was recited", in which a one way decryption is explicitly defined as a token that cannot be decrypted is not taught by Bachman et al. The Examiner continues to maintain the position that Bachman fails to disclose a token encrypted in an undecryptable manner as agreed in the telephonic interview of 4/8/04.

However, upon further search and consideration of the prior art, Applicant's arguments with respect to the amended claims have been considered but are moot in view of the new ground(s) of rejection.

Wilf(abstract) discloses "a token for session management over a stateless protocol" that "is formed by digitally hashing a plurality of identifiers contained in a request."

Wilf(Column 3, lines 51- Column 4, line 4) discloses a digital hash, created through a plurality of methods including the well known MD5 algorithms. The Examiner notes that the Applicant produces the one-way encryption token through this methodology as well. Applicant's recent amendments to the specification include page 24, line 7.

"Examples of one-way encryption schemes that may be used with the exemplary implementation of the session-state manager include a 128-bit MD5 hash, Secure Hash Algorithm(SHA), or any other cryptographically strong one-way hash function. The preferred one-way encryption scheme is fast and produces results that are apparently randomly distributed."

***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3, 7-8, 12, 16, 19-20, 27, 34, 39, 42-44, 48-50 are rejected under 35 U.S.C. 103(a) as being anticipated by Wilf.

Claims 4-6, 9-11, 13-14, 21-23, 26, 28-33, 35, 40-41, 47 are rejected under 35 U.S.C. 103(a) as being anticipated by Wilf and Bachman et. al.

In reference to claim 1:

Wilf discloses a session state management method comprising:

Generating an encoded session-state token, wherein the token incorporates a representation of session state of a client. (Column 4, lines 5-35)

Encrypting the encoded token to produce an encrypted token that cannot be decrypted. (Column 3, lines 52- Column 4, line 4)

Wilf fails to explicitly disclose a method comprising sending the encrypted token to the client. The Examiner takes official notice that sending a token for use in a state-management method to the client was well known in the art. Cookies for example, are messages sent to browsers to track the state of a client. The advantage in using cookies, is that it takes the burden off the server to maintain the tokens of its clients.

Wilf(Column 1, lines 60 – Column 2, line 6) further discloses this method in the prior art. Wilf (Column 4, lines 15-25) also discloses that the session identifier is taking the form of a cookie. This is also disclosed in US patent 6,041,357 Kunzelman, Figure 2.

It would have been obvious to one of ordinary skill in the art at the time of invention, to send the encrypted token/cookie to the client so that the clients would keep track of their individual sessions, lessening the computational and storage burden of the server.

In reference to claim 2:

Wilf (Column 4, lines 40-65) discloses a method further comprising authenticating the user of the client, where the authenticating the user comprises collecting data and a response to authenticate the user with a digital fingerprint.

In reference to claim 3:

Wilf discloses a method as recited in claim 1, further comprising authenticating the user of the client, wherein the authenticating step comprises:

- Receiving a user identification indicator("username") and a password (Column 6, lines 4-8) & (Figure 3 step 4)

- Establishing a session for a user, where the session of the user is establish and the server begins to service the HTTP requests of the client. (Column 6, lines 28-32)

Wilf fails to explicitly disclose

- Comparing the username to a database of authorized user records, each record containing a username and a user-name associated password
- Comparing the password received in the receiving step to a username associated password of a record containing a matching username and

The examiner takes official notice that it was well known in the art to compare the username to a database of authorized records, and comparing the password to a database of authorized records.

In order to verify that a password and username is valid, one would need to verify received username/password info, against an official record of it.

It would have been obvious to one of ordinary skill in the art at the time of invention to compare the received username and password in Wilf to a record of usernames and passwords in a database, in order to verify the actual identity of the current user who entered the password.

In reference to claim 4:

Wilf fails to explicitly disclose a method wherein the generating step comprises forming a confirmation token that incorporates a representation of an incremental time block

- Bachman(Column 4, lines 10-37) & (Column 6, lines 10-19) discloses a method as recited in claim 1, wherein the generating step comprises forming a confirmation token that incorporates a representation of an incremental time block
- Bachman (Column 4, line 32-36) discloses that using the method to compare the tokens with an established page transmission time T included allows the system to recognize when a session has expired.

It would have been obvious to one of ordinary skill in the art at the time of invention to apply the use of Bachman's session expiration mechanism to the session management token of Wilf in order to be able to determine whether or not the session for a particular user had expired.

In reference to claim 5:

Wilf fails to explicitly disclose a method wherein the generating step comprises forming a confirmation token that incorporates a representation of a current incremental time block

- Bachman(Column 4, lines 10-37) & (Column 6, lines 10-19) discloses a method as recited in claim 1, wherein the generating step comprises forming a confirmation token that incorporates a representation of a current incremental time block
- Bachman (Column 4, line 32-36) discloses that using the method to compare the tokens with an established page transmission time T included allows the system to recognize when a session has expired.

It would have been obvious to one of ordinary skill in the art at the time of invention to apply the use of Bachman's session expiration mechanism to the session management token of Wilf in order to be able to determine whether or not the session for a particular user had expired.

In reference to claim 6:

Wilf fails to explicitly disclose a method wherein the generating step comprises forming a confirmation token that incorporates a representation of an incremental time block that is prior a current incremental time block.

- Bachman(Column 4, lines 10-37) & (Column 6, lines 10-19) discloses a method as recited in claim 1, wherein the generating step comprises forming a confirmation token that incorporates a representation of an incremental time block that is prior a current incremental time block, where the current time block is the current session token, and the prior incremental time block was the previously logged time on the client when the session was first established.

Bachman (Column 4, line 32-36) teaches that using the method to compare the tokens with an established page transmission time T included allows the system to recognize when a session has expired.

It would have been obvious to one of ordinary skill in the art at the time of invention to apply the use of Bachman's session expiration mechanism to the session management token of Wilf in order to be able to determine whether or not the session for a particular user had expired.

Claim 7 is rejected for the same reasons as claim 1.

In reference to claim 8:

A session state management method comprising:

Wilf discloses generating an encrypted, confirmation session-state token that cannot be decrypted, where a token is generated based on the user identifiers within the token. (Column 4, lines 48-53)

Wilf discloses comparing the confirmation token with the received token, wherein the confirmation token is compared to determine if it exists within the database. (Column 4, lines 58-65) & (Column 4, lines 30-35)

Wilf fails to explicitly disclose a receiving an encrypted session state token that cannot be decrypted from a client, wherein the token incorporates a representation of session state of a client.

The examiner takes official notice that receiving tokens in session state management methods from the client was well known in the art.

Wilf (Column 2, lines 5-6) discloses an example of this

Receiving a token from a client is also a necessary consequence of having the client maintain it's own state information. At some point, the information would need to be sent back to the server.

It would have been obvious to one of ordinary skill in the art at the time of invention to receive tokens in session state management protocols from the client to process the session state information maintained by the client, where the maintaining the session token by the client would be performed in order to give the advantage of lightening the computational load on the server.

Claim 9 is rejected for the same reasons as claim 4.

Claim 10 is rejected for the same reasons as claim 5.

Claim 11 is rejected for the same reasons as claim 6.

Claim 12 is rejected for the same reasons as claim 1.

Claim 13 is rejected for the same reasons as claim 5.

Claim 14 is rejected for the same reasons as claim 5.

Claim 15 is allowable as previously stated.

Claim 16 is rejected for the same reasons as claim 8.

Claim 17 is allowable as previously stated.

Claim 18 is allowable as previously stated.

Claim 19 is rejected for the same reasons as claim 2.

Claim 20 is rejected for the same reasons as claim 3.

Claim 21 is rejected for the same reasons as claim 23.

Claim 22 is rejected for the same reasons as claim 23.

In reference to claim 23:

Wilf discloses a session state management method using an encoded token comprising:

- Encrypting the encoded token to produce an encrypted token that cannot be decrypted.
- (Column 3, lines 52- Column 4, line 4)
- The user is identified by a user identification indicator (UserID) (Column 6, lines 5-7)

Wilf fails to disclose a method wherein:

- A time block is identified by a time block identification indicator (TimeID), Figure 5 "timeoutID"(near <BODY onLoad=""> )
- The generating step comprises forming a session state token at least partially based upon the UserID and the TimeID. (Column 3, lines 43-49)

Bachman et al. discloses a method wherein:

- The user is identified by a user identification indicator (UserID) (Figure 4, Item 405)
- A time block is identified by a time block identification indicator (TimeID), Figure 5 "timeoutID"(near <BODY onLoad=""> )
- The generating step comprises forming a session state token at least partially based upon the UserID and the TimeID. (Column 3, lines 43-49)

Bachman (Column 4, line 32-36) teaches that using the method to compare the tokens with an established page transmission time T included allows the system to recognize when a session has expired.

It would have been obvious to one of ordinary skill in the art at the time of invention to apply the use of Bachman's session expiration mechanism to the session management token of Wilf in order to be able to determine whether or not the session for a particular user had expired.

Claims 24-25 have been canceled.

Claim 26 is rejected for the same reasons as claim 23.

Claim 27 is rejected for the same reasons as claim 2.

Claim 28 is rejected for the same reasons as claim 23.

In reference to claim 29:

Bachman et al. discloses a method wherein the combining step comprises concatenating UserID and TimeID, where the concatenation is performed in both the step of storing the ID's together in the index table of the token and, when the token is placed in the hypertext link in the page. (Column 3, lines 43-64)

In reference to claim 30:

Bachman et al. discloses a method wherein the combining step comprises concatenating UserID, TimeID, and a code key, where the code key is the random numbers used in the generation of the token. (Column 3, lines 34-49)

In reference to claim 31:

Wilf(Column 3, lines 52- Column 4, line 4) discloses a method as recited in claim 28, wherein the encrypting step comprises encrypting the encoded token using a one-way encryption method.

In reference to claim 32:

Bachman et al. discloses a method wherein the encrypting step comprises:

Encrypting the encoded token using a one-way encryption scheme to produce an encrypted result. (Column 5, lines 53-56)

Selecting a defined portion of the encrypted result to form a session-state token. (Column 5, line 64 – Column 6, line 9)

Claim 33 is rejected for the same reasons as claim 23.

Claim 34 is rejected for the same reasons as claim 8.

In reference to claim 35:

Wilf discloses a session state management method using an encoded token,

but fails to explicitly disclose a session-state management method wherein the generating step comprises forming a confirmation token that incorporates a representation of a current incremental time block, if confirmation and received tokens fail to match, further comprising:

- Generating a new confirmation token using a representation of a incremental time block previous of the time block representation used for the previous generating step
- Comparing the new confirmation token with the received token.

Bachman et al. discloses a method wherein the generating step comprises forming a confirmation token that incorporates a representation of a current incremental time block, if confirmation and received tokens fail to match, further comprising:

- Generating a new confirmation token using a representation of a incremental time block previous of the time block representation used for the previous generating step, where the

new confirmation token is generated using a representation of the previous time block that existed in the previous token. (Column 6, lines 20-28)

- Comparing the new confirmation token with the received token. (Column 6, lines 27-31)

Bachman (Column 4, line 32-36) teaches that using the method to compare the tokens with an established page transmission time T included allows the system to recognize when a session has expired.

It would have been obvious to one of ordinary skill in the art at the time of invention to apply the use of Bachman's session expiration mechanism to the session management token of Wilf in order to be able to determine whether or not the session for a particular user had expired.

Claim 36 is allowable as previously indicated.

Claims 37 – 38 have been canceled.

Claim 39 is rejected for the same reasons as claim 8.

In reference to claim 40:

Wilf discloses a session state management method using an encoded token but fails to explicitly disclose a session-state management method comprising:

- Receiving a user-associated TimeID from a client, wherein the encoded token incorporates a representation of session-state of the user's session.
- Designating a first time block identification indicator (TimeID) for a first time block.

- Comparing the user-associated TimeID with the first TimeID.

Bachman et al. discloses a session-state management method comprising:

- Receiving a user-associated TimeID from a client, wherein the encoded token incorporates a representation of session-state of the user's session, where the received TimeID is the Time T encoded within the client's token sent back to the server when the user peruses a page. (Column 4, lines 11-37)
- Designating a first time block identification indicator (TimeID) for a first time block, where the first time block identification indicator is stored on the server and indicates the current time. (Column 4, lines 11-37)
- Comparing the user-associated TimeID with the first TimeID, where the user associated current time t is compared with the original timeID T. (Column 4, lines 11-37)

Bachman (Column 4, line 32-36) teaches that using the method to compare the tokens with an established page transmission time T included allows the system to recognize when a session has expired.

It would have been obvious to one of ordinary skill in the art at the time of invention to apply the use of Bachman's session expiration mechanism to the session management token of Wilf in order to be able to determine whether or not the session for a particular user had expired.

In reference to claim 41:

Bachman et al. discloses a method further comprising:

- Designating a prior TimeID for a time block prior to the first time block, where the prior TimeID is the time T stored on the user's token, received by the server when the user peruses a page. This TimeID is inherently prior to first time block containing the current time. (Column 4, lines 11-37)
- Comparing the user-associated TimeID with the prior TimeID. (Column 4, lines 11-37)

Claim 42 is substantially similar to claim 1 and is rejected for the same reasons.

Claim 43 is substantially similar to claim 8 and is rejected for the same reasons.

Claim 44 is substantially similar to claim 2 and is rejected for the same reasons.

Claim 47 is substantially similar to claim 23 and is rejected for the same reasons.

Claim 48 is substantially similar to claim 8 and is rejected for the same reasons.

Claim 49 is rejected for the same reasons as claim 1.

Claim 50 is rejected for the same reasons as claim 8.

***Conclusion***

5. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of the final action and the advisory action is not mailed under after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension pursuant to 37 CFR 1.136(A) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas M Ho whose telephone number is (703)305-8029. The examiner can normally be reached on M-F from 8:30am – 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached at (703)308-4789. The fax phone numbers for the organization where this application or proceeding is assigned are (703)746-7239 for regular communications and (703)746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)306-5484.

TMH

July 30th, 2004

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100